CRYPTOGRAPHY AND NETWORK SECURITY
(MCAP 3160)

Time Allotted : 3 hrs **Full Marks : 70**

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and any 5 (five) from Group B to E, taking at least one from each group.

Candidates are required to give answer in their own words as far as practicable.

Group – A
(Multiple Choice Type Questions)

1. Choose the correct alternative for the following: **10 × 1 = 10**

(i) Message _____ means that the receiver is ensured that the message is coming from the intended sender, not an imposter.
(a) confidentiality (b) integrity
(c) authentication (d) none of the above

(ii) What is 11 mod 7 and -11 mod 7?
(a) 4 and 5 (b) 4 and 4 (c) 5 and 3 (d) 4 and 3.

(iii) If ϕ denotes Euler's totient function, then value of $\phi(37)$ is
(a) 24 (b) 37 (c) 36 (d) 1.

(iv) DES uses a key generator to generate sixteen _____ round keys.
(a) 32-bit (b) 48-bit (c) 54-bit (d) 42-bit

(v) Which one of the following is not a public key distribution technique?
(a) Public-key certificates (b) Hashing certificates
(c) Publicly available directories (d) Public-key authority.

(vi) In RSA, we select a value 'e' such that it lies between 0 and Φ(n) and it is relatively prime to Φ(n).
(a) True (b) False (c) Maybe (d) Can't be said.

(vii) In _____, there is a single path from the fully trusted authority to any certificate.
(a) X.509 (b) PGP (c) KDC (d) none of the above

(viii) The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not
(a) authenticated (b) joined
(c) submit (d) separate.

(ix) A proxy firewall filters at the
(a) physical layer (b) application layer
(c) data link layer (d) network layer.

(x) "Fraud access points are created to access information such as passwords" - what wireless network threat is this?
(a) Identity theft (b) Network injection
(c) Man in the middle attack (d) Malicious association.

Group – B

2. (a) List five basic properties of a good encryption algorithm.

(b) Which principle of security is breached because of masquerade?

(c) Give an example of replay attacks. Why are they considered to be fatal?

4 + 4 + 4 = 12

3. (a) Use Euclidean algorithm to determine gcd (4655, 12075).

(b) Prove the following: [(a mod n) (b mod n)] mod n = (a b) mod n.

(c) State Fermat's Little Theorem.

5 + 5 + 2 =12

Group – C

4. (a) Briefly explain the Playfair cipher with an example.

(b) What is the difference between a block cipher and a stream cipher?

(c) Explain the avalanche effect.

6 + 3 + 3 = 12

5. (a) Explain how Vernam cipher works by enciphering the following text "V E R N A M C I P H E R" using the: 76 48 16 82 44 3 58 11 60 5 48 88.

(b) What is a meet-in-the-middle attack in context of double DES?

9 + 3 = 12

Group – D

6. (a) Perform encryption and decryption using the RSA algorithm, for the following: p = 3; q = 11, e = 7; M = 5.

(b) Explain factoring attack and timing attack on RSA.

6 + (3 + 3) = 12

CRYPTOGRAPHY AND NETWORK SECURITY
(MCAP 3160)

Time Allotted : 3 hrs **Full Marks : 70**

Figures out of the right margin indicate full marks.

Candidates are required to answer Group A and any 5 (five) from Group B to E, taking at least one from each group.

Candidates are required to give answer in their own words as far as practicable.

Group – A
(Multiple Choice Type Questions)

1. Choose the correct alternative for the following: **10 × 1 = 10**

(i) Message _____ means that the receiver is ensured that the message is coming from the intended sender, not an imposter.
(a) confidentiality (b) integrity
(c) authentication (d) none of the above

(ii) What is 11 mod 7 and -11 mod 7?
(a) 4 and 5 (b) 4 and 4 (c) 5 and 3 (d) 4 and 3.

(iii) If ϕ denotes Euler's totient function, then value of $\phi(37)$ is
(a) 24 (b) 37 (c) 36 (d) 1.

(iv) DES uses a key generator to generate sixteen _____ round keys.
(a) 32-bit (b) 48-bit (c) 54-bit (d) 42-bit

(v) Which one of the following is not a public key distribution technique?
(a) Public-key certificates (b) Hashing certificates
(c) Publicly available directories (d) Public-key authority.

(vi) In RSA, we select a value 'e' such that it lies between 0 and Φ(n) and it is relatively prime to Φ(n).
(a) True (b) False (c) Maybe (d) Can't be said.

(vii) In _____, there is a single path from the fully trusted authority to any certificate.
(a) X.509 (b) PGP (c) KDC (d) none of the above

(viii) The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not
(a) authenticated (b) joined
(c) submit (d) separate.

(ix) A proxy firewall filters at the
(a) physical layer (b) application layer
(c) data link layer (d) network layer.

(x) "Fraud access points are created to access information such as passwords" - what wireless network threat is this?
(a) Identity theft (b) Network injection
(c) Man in the middle attack (d) Malicious association.

Group – B

2. (a) List five basic properties of a good encryption algorithm.

(b) Which principle of security is breached because of masquerade?

(c) Give an example of replay attacks. Why are they considered to be fatal?

4 + 4 + 4 = 12

3. (a) Use Euclidean algorithm to determine gcd (4655, 12075).

(b) Prove the following: [(a mod n) (b mod n)] mod n = (a b) mod n.

(c) State Fermat's Little Theorem.

5 + 5 + 2 =12

Group – C

4. (a) Briefly explain the Playfair cipher with an example.

(b) What is the difference between a block cipher and a stream cipher?

(c) Explain the avalanche effect.

6 + 3 + 3 = 12

5. (a) Explain how Vernam cipher works by enciphering the following text "V E R N A M C I P H E R" using the: 76 48 16 82 44 3 58 11 60 5 48 88.

(b) What is a meet-in-the-middle attack in context of double DES?

9 + 3 = 12

Group – D

6. (a) Perform encryption and decryption using the RSA algorithm, for the following: p = 3; q = 11, e = 7; M = 5.

(b) Explain factoring attack and timing attack on RSA.

6 + (3 + 3) = 12

7. (a) What is a public-key certificate? What are the requirements for the use of a public-key certificate scheme?

   (b) Briefly explain the man-in-the-middle attack on Diffie-Hellman key exchange protocol.

   (c) What requirements should a digital signature scheme satisfy?

(2 + 3) + 4 + 3 = 12

Group – E

8. (a) What are the four requirements for Kerberos? What entities constitute a full-service Kerberos environment?

   (b) What is the purpose of the X.509 standard? What are the key elements of an X.509 certificate?

4 + (2 + 6) = 12

9. (a) What are the five principal services provided by PGP?

   (b) Why is it necessary to separate wireless networks from wired networks in an organization? How is it accomplished?

   (c) What is the role of Merkle tree in blockchains?

4 + (3 + 3) + 2 = 12